# Intercept-resend attacks on Semiquantum secret sharing and the Improvements

Jason Lin, Chun-Wei Yang, Chia-Wei Tsai, and Tzonelih Hwang*

**Abstract**

Recently, Li et al. [Phys. Rev. A, 82(2), 022303] presented two semi-quantum secret sharing (SQSS) protocols using GHZ-like states. The proposed schemes are rather practical because only the secret dealer requires to equip with advanced quantum devices such as quantum memory, whereas the other agents can merely perform classical operations to complete the secret sharing. However, this study points out that a security pitfall exists in the eavesdropping check phase of both schemes that could mount to an Intercept-resend attack and a Trojan horse attack on the two schemes, respectively, to disclose the other agent's shadow, and further to reveal the master key of the SQSS, which contradicts to the security requirement of a QSS. Fortunately, two possible solutions are proposed to avoid this security pitfall.

***keywords:*** Quantum secret sharing, GHZ-like state, Intercept-resend attack, Trojan horse attack

## 1 Introduction

Since the first quantum secret sharing (QSS) protocol was presented by Mark et al.'s via triplet Greenberger-Horne-Zeilinger (GHZ) state in 1999 [1], lots of QSS schemes have also been proposed [2-13]. The main goal of a QSS is to distribute a secret among several agents based on the quantum mechanics. Only when enough subsets of legitimate agents cooperate can the

*Corresponding Author

secret be recovered. On the contrary, any agent alone is not able to acquire the dealer's secret by his/her own shadow. A secure QSS should be able to avoid the attack from both an outside eavesdropper and an inside malicious user.

Recently, Li et al. proposed two novel semi-quantum secret sharing (SQSS) protocols via triplet GHZ-like state [13]. According to their definition, the term "semi-quantum" implies that the secret dealer is a powerful quantum server, whereas the other agents are all classical clients. More precisely, the secret dealer has the ability to perform the following operations: (1) preparing GHZ-like state, (2) performing the Bell measurement and the three-qubit joint measurement, (3) storing photons in a short-term quantum memory. As for the classical agents, they are restricted to perform the following operations over the quantum channel: (1) preparing new qubits in the classical basis $\{|0\rangle, |1\rangle\}$, (2) measuring photons in the classical basis, (3) reordering the photons via different delay lines, (4) sending or reflecting the qubits without disturbance. Since the classical basis only considers the qubit $|0\rangle$ and $|1\rangle$, the other quantum superpositions of single photon are not included here. Therefore, the agents' operations above are equivalent to the traditional {0, 1} computation.

The two protocols proposed by Li et al. [13] are namely the randomization-based SQSS and the measure-resend SQSS, respectively. Both schemes are based on the entanglement correlation of GHZ-like state $|\psi'\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|\phi^+\rangle + |1\rangle|\psi^+\rangle)$, which can be easily generated by performing the Hadamard gate $H$ $(= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|))$ on each qubit of the standard GHZ state $|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Under the three-party QSS scenario, it can be seen that if each party holds the *1st*, the *2nd*, and the *3rd* particle of a GHZ-like state, respectively, then their classical-basis measurements (say $MR_1$, $MR_2$, and $MR_3$) will agree to a secret sharing relationship: $MR_1 = MR_2 \oplus MR_3$, where the measurement result is encoded as '0' if $|0\rangle$, '1' if $|1\rangle$.

However, this study attempts to show that under the three-party scenario (i.e., one boss and two agents) of Li et al.'s scheme, a malicious agent is possible to launch an Intercept-resend attack on the randomization-based SQSS and a Trojan horse attack [14, 15, 16, 17] on the measure-resend SQSS to reveal the other agent's shadow. This contradicts to the security requirements of a QSS. Fortunately, the above problems can be respectively solved by a carefully designed eavesdropping check process and the use of some special optical devices that filter out the spy photons of the Trojan horse attacks.

The rest of this paper is constructed as follows. Section 2 reviews Li et al.'s two SQSS schemes via GHZ-like state. Section 3 points out the problem and gives two solutions to remedy the loophole. Finally, Section 4 gives a brief conclusion to the result.

## 2 Review of Li et al.'s SQSS schemes

In this section, a brief review of Li et al.'s two SQSS schemes is given. The only difference between these two schemes is the definition of the classical agent's ability. For a randomization-based SQSS protocol, classical agents are limited to perform operations: (2), (3), and (4), while in a measure-resend protocol, classical agents are limited to perform operations: (1), (2), and (4), as defined in Sec. 1.

### 2.1 Randomization-based SQSS protocol

In this subsection, the SQSS is considered under a three-party scenario as follows. Suppose a boss Alice wants to share a secret with her two agents: Bob and Charlie. She splits her secret key $K_A$ into two pieces of shadow key: $K_B$ and $K_C$, which will deliver to Bob and Charlie, respectively. Only when Bob and Charlie collaborate can $K_A$ be recovered. The procedure of the randomization-based SQSS can be described in the following steps:

**Step 1.** Alice first prepares $N$ triplet GHZ-like states all in $|\psi'\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle)$. Here, the quantum states $\{|0\rangle, |1\rangle\}$ can be classically measured by $Z$ basis. Then, she divides these $N$ GHZ-like states into three sequences $S_A$, $S_B$, and $S_C$, which include the *1st*, the *2nd*, and the *3rd* particles of all GHZ-like states, respectively. After the above preparation, Alice retains the quantum sequence $S_A$, and sends the sequence $S_B$ to Bob, $S_C$ to Charlie.

**Step 2.** When Bob and Charlie receive the photons, respectively, they choose to adopt either the SHARE mode or the CHECK mode on each qubit, respectively. In the SHARE mode, the agent performs a $Z$-basis measurement on the qubit, whereas in the CHECK mode, the agent reflects the qubit back to Alice. Notice that those returned qubits in the CHECK mode are reordered via different delay lines.

**Step 3.** Alice stores the reflected qubits from Bob and Charlie in a short-term quantum memory, and publicly announces the reception of these photon sequences. After that, Bob and Charlie publish the correct order of the reflected qubits, and their original positions in the sequences delivered by Alice, respectively. According to the agents' reports, Alice can recover the reflected qubits into the correct order.

**Step 4.** For each GHZ-like state, both Bob and Charlie announce their decisions respectively on the corresponding two particles of $S_B$ and $S_C$, which can be one of the four cases as shown in Table 1. Then, Alice can perform one of the four actions on the corresponding qubits as depicted in Table 1.

**Step 5.** For the eavesdropping check, those qubits in cases (2), (3), and (4) of Table 1 are publicly discussed. The involved parties have to publish their measurement results in those cases to see whether each corresponding three qubits is consistent to the correlation of a GHZ-like state $|\psi'\rangle$ $(= \frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|\phi^+\rangle + |1\rangle|\psi^+\rangle))$. If the error rate is higher than a predetermined threshold, then Alice terminates the protocol and restarts from Step 1. Otherwise, the protocol continues to the next step.

**Step 6.** As for the secret sharing policy in the case (1) of Table 1, the *1st*, the *2nd*, and the *3rd* qubits of GHZ-like states are measured by Alice, Bob, and Charlie, respectively, using $Z$-basis. They can transform these measurement results into three binary bit sequences, in which the result is '0' if $|0\rangle$ and '1' if $|1\rangle$. After the transformation, Alice, Bob, and Charlie will obtain a key bit string $K_A$, $K_B$, and $K_C$, respectively, which conform to the secret sharing relationship, i.e., $K_A = K_B \oplus K_C$.

Table 1: The actions taken by the secret dealer Alice in each case.

| Case | Bob | Charlie | Alice |
|---|---|---|---|
| (1) | SHARE | SHARE | ACTION (i) |
| (2) | SHARE | CHECK | ACTION (ii) |
| (3) | CHECK | SHARE | ACTION (iii) |
| (4) | CHECK | CHECK | ACTION (iv) |

**(i):** Alice measures her own qubit with $Z$-basis.

**(ii):** Alice performs Bell measurement on her qubit and Charlie's returned qubit.

**(iii):** Alice performs Bell measurement on her qubit and Bob's returned qubit.

**(iv):** Alice performs an appropriate three-qubit joint measurement on her qubit and the returned qubits.

The randomization-based SQSS protocol uses the entanglement correlation of GHZ-like state $|\psi'\rangle$ to achieve the goal of secret sharing. In this type of protocol, the agents will directly perform $Z$-basis measurement on the photons in the SHARE mode. Conversely, by modifying the operations performed by the agents, Li et al. further proposed the other scheme called the measure-resend SQSS protocol, which will be described in Sec. 2.2.

## 2.2 Measure-resend SQSS protocol

Similar to Sec. 2.1, the measure-resend SQSS scheme is also reviewed under a three-party scenario (i.e., a boss Alice, and two agents: Bob and Charlie). The modified steps (*) are depicted in detail as follows. The other steps are the same as those described in Sec. 2.1 and thus are omitted here.

**(*Step 2)** There are two modes (i.e., SHARE and CHECK) that Bob and Charlie can decide to perform on each received photon. For the CHECK mode, the agent still reflects the qubit back to Alice via different delay lines similar to Sec. 1. On the contrary, in the SHARE mode, the agent measures the received qubits in $Z$-basis, and returns a sequence of newly generated photons of the same states to Alice.

**(*Step 3)** Alice stores the photon sequences reflected from Bob and Charlie in a short-term quantum memory, and publicly confirms the reception of them. Subsequently, Bob and Charlie declare the positions of particles being measured and being reflected.

**(*Step 4)** According to the agents' reports, Alice can perform one of the four actions on her own qubit and the corresponding qubits as depicted in Table 1.

The measure-resend SQSS protocol is also based on the entanglement correlation of the GHZ-like state $|\psi'\rangle$. The only difference between these two schemes (the randomization-based SQSS and the measure-resend SQSS) is the type of operations allowed to perform by the agent in the SHARE mode. Considering the eavesdropping check, both schemes discuss the measurement result of each qubit in the GHZ-like state to detect the presence of eavesdroppers. However, this check strategy may not be able to prevent Bob or Charlie from maliciously launching attacks on the SQSS protocols. More details of the attacks will be discussed in Sec. 3.

# 3 Attacks and the improvements

This section shows that under the three-party scenario (i.e., one boss and two agents) of Li et al.'s scheme, a malicious agent is possible to launch an Intercept-resend attack on the randomization-based SQSS and a Trojan horse attack [14, 15, 16, 17] on the measure-resend SQSS to reveal the other agent's shadow and further to derive Alice's secret key. This contradicts to the security requirements of a QSS. Fortunately, the above problems can be respectively solved by a carefully designed eavesdropping check process and the use of some special optical devices that filter out the spy photons of the Trojan horse attacks.

## 3.1 Attacks on Li et al.'s SQSS schemes

Both Bob and Charlie can act as a dishonest insider to derive Alice's shared secret. In general, an eavesdropper is assumed to be powerful enough to equip with any quantum devices.

### 3.1.1 The Intercept-resend attack on the randomization-based SQSS.

Suppose that Bob is a dishonest insider. He first intercepts the photon sequence $S_C$ (from Alice to Charlie) in Step 1, and stores it in his quantum memory. Then, he prepares a new photon sequence $S_E$ randomly chosen from $|0\rangle$ or $|1\rangle$, and sends it to Charlie, where $S_E$ is of the same length as $S_C$. Notice that the wavelength of each photon in $S_E$ is set to be different from the others so that Bob is alble to identify their individual position.

When Charlie receives the sequence $S_E$ in Step 2, he will perform $Z$-basis measurement on those photons chosen for the SHARE mode, and reflect the ones that are chosen for the CHECK mode via different delay lines. At this time, Bob can intercept the reflected sequence (from Charlie to Alice), and replace those photons with the corresponding photons in $S_C$ and then send them back to Alice. Bob is able to do so by distinguishing the wavelengths of the reflected photons from Charlie.

Later, Bob deliberately selects the SHARE mode on those photons in $S_B$ that their corresponding photons in $S_C$ have been chosen by Charlie as in the SHARE mode, and randomly select SHARE or CHECK on the other photons in $S_B$. The above action is to avoid the presence of the case (3) in Table 1 because it has a 50% probability of being detected. More precisely, since all the SHARE photons measured by Charlie are the forged photons in $S_E$, there is a 50% probability on each three-particle set of the case (3) that will not follow the entanglement correlation of GHZ-like state $|\psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\phi^+\rangle + |1\rangle|\psi^+\rangle)$.

For the eavesdropping check, Bob can escape from detection because of all the reflected photons in cases (1), (2), and (4) of Table 1 are indeed generated by Alice. Therefore, he can obtain Charlie's shadow $K_C$ by measuring the SHARE photons in $S_C$, and further derive Alice's secret key with $K_B \oplus K_C = K_A$.

### 3.1.2 The Trojan-horse attack on the measure-resend SQSS.

Let us also assume here that Bob is a malicious insider. He first attaches some invisible photons $S_T$ on each particle of $S_C$ transmitted from Alice to Charlie in Step 1, and then inserts some delay photons $S_D$ in the same time window to each particle of $S_C$. Notice that the wavelength in each photon of $S_D$ is set to be the same as the corresponding photon in $S_C$, whereas the wavelength in each photon of $S_T$ is close to the corresponding photon in $S_C$.

When Charlie receives the sequence $S_C$ in Step 2, he measures those photons in the SHARE mode with $Z$-basis, and returns a sequence of newly generated photons of the same states to Alice. The corresponding photons of the SHARE photons in $S_T$ and $S_D$ will vanish after the replacement of the newly produced photons. As for the CHECK photons, Charlie will directly reflect them without any reordering operation to Alice. At this time, Bob can intercept the returned sequence (from Charlie to Alice), and perform $Z$-basis measurement on those photons that their corresponding spy photons have disappeared.

After the measurement, Bob resends the returned sequence back to Alice without any further action. Since Alice will also perform $Z$-basis measurement on the SHARE photons of Charlie in Step 4, the measurement results will not be different from the ones measured by Bob. Hence, the three cases (1), (2), and (3) in Table 1 used for the eavesdropping check will not detect the attack. Bob can obtain Charlie's shadow $K_C$ by those $Z$-basis measurement results of the SHARE photons in the case (4) of Table 1 and further derive Alice's secret key with $K_B \oplus K_C = K_A$.

## 3.2 Possible solutions for the attacks

Two solutions to avoid the attacks are proposed here. The first one is to set a new threshold of eavesdropping check in the randomization-based SQSS. The second solution is to equip with some special optical filter devices to detect the Trojan horse attacks on the measure-resend SQSS.

**Solution 1.** A new threshold for the eavesdropping check.

In Table 1, all four cases should be evenly distributed. However, if Bob performs the intercept-resend attack as shown in Sec. 3.1.1, there is no chance for case (3) of Table 1 to appear. Thus, to prevent this attack, before the eavesdropping check of Step 5, Alice can first calculate the occurrence $\rho$ of case (3) in Table 1, and decide the existence of the attack. If $\rho$ is too small, then Alice can abort the protocol.

**Solution 2.** Agents install some optical filter devices.

Since the attack in Sec. 3.1.2 is based on the spy photons in the Trojan horse attacks, when Charlie receives the photons in Step 2, he can equip with some special optical devices such as the wavelength quantum filter and the photon number splitters (PNS) to detect the attacks. According to [14, 15, 16, 17], the wavelength quantum filter can eliminate the invisible photons attached on the legitimate ones, and the PNS can spit each legitimate particle to discover the delay photons. If there is an irrational high rate of multi-photon signal, then Charlie announces to restart the protocol from Step 1.

## 4 Conclusions

This paper has pointed out two attacks on both of Li et al.'s SQSS schemes, respectively. Under the three-party scenario (i.e., one boss and two agents), a malicious insider could possibly launch the Intercept-resend attack on the randomization-based SQSS and the Trojan horse attacks on the measure-resend SQSS to obtain the other agent's shadow, which can also lead to derive the boss's secret key. Fortunately, two solutions are given in this paper to avoid the attacks (i.e., one is to add a new threshold for the eavesdropping check, and the other is to equip with some special optical devices to filter out the spy photons). With the second solution, since near a half of the transmitted photons are used in devices to detect the Trojan horse attack for each agent, the qubit efficiency will be seriously jeopardized. Hence, how to design a QSS protocol which is congenitally free from this attack is a promising future research.

## Acknowledgement

We would like to thank the National Science Council of the Republic of China, Taiwan for partially supporting this research in finance under the Contract No. NSC 98-2221- E-006-097-MY3.

## References

[1] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," Phys. Rev. A, vol. 59, no. 3, pp. 1829-1834, (1999).

[2] D. Gottesman, "Theory of quantum secret sharing," Phys. Rev. A, vol. 61, no. 4, id. 042311, (2000).

[3] G.P. Guo and G.C. Guo, “Quantum secret sharing without entanglement,” Phys. Lett. A, vol. 310, no. 4, pp. 247-251, (2003).

[4] L. Xiao, G.L. Long, F.G. Deng, and J.W. Pan, “Efficient multiparty quantum-secret-sharing schemes,” Phys. Rev. A, vol. 69, no. 5, id. 052307, (2004).

[5] L.Y. Hsu and C.M. Li, “Quantum secret sharing using product states,” Phys. Rev. A, vol. 71, no. 2, id. 022321, (2005).

[6] Z.J. Zhang and Z.X. Man, “Multiparty quantum secret sharing of classical messages based on entanglement swapping,” Phys. Rev. A, vol. 72, no. 2, id. 022303, (2005).

[7] F.G. Deng, G.L. Long, and H.Y. Zhou, “An efficient quantum secret sharing scheme with Einstein-Podolsky-Rosen pairs,” Phys. Lett. A, vol. 340, no. 1-4, pp. 43-50, (2005).

[8] F.G. Deng, X.H. Li, and H.Y. Zhou, “Efficient high-capacity quantum secret sharing with two-photon entanglement,” Phys. Lett. A, vol. 372, no. 12, pp. 1957-1962, (2008).

[9] Y. Sun, Q.Y. Wen, F. Gao, X.B. Chen, and F.C. Zhu, “Multiparty quantum secret sharing based on Bell measurement,” Opt. Commun., vol. 282, no. 17, pp. 3647-3651, (2009).

[10] J.H. Chen, K.C. Lee, and T. Hwang, “The enhancement of Zhou et al.’s quantum secret sharing protocol,” Int. J. Mod. Phy. C, vol. 20, no. 10, pp. 1531-1535, (2009).

[11] R.H. Shi, L.S. Huang, W. Yang, and H. Zhong, “Multiparty quantum secret sharing with Bell states and Bell measurements,” Opt. Commun., vol. 283, no. 11, pp. 2476-2480, (2010).

[12] C.R. Hsieh, C.W. Tsai, and T. Hwang, “Quantum secret sharing using GHZ-like state,” Commun. Theor. Phys., vol. 54, no. 6, pp. 1019-1022, (2010).

[13] Q. Li, W.H. Chan, and D.Y. Long, “Semiquantum secret sharing using entangled states,” Phys. Rev. A, vol. 82, no. 2, id. 022303, (2010).

[14] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys., vol. 74, no. 1, pp. 145-195, (2002).

[15] F.G. Deng, X.H. Li, H.Y. Zhou, and Z.J. Zhang, “Improving the security of multiparty quantum secret sharing against Trojan horse attack,” Phys. Rev. A, vol. 72, no. 4, id. 044302, (2005).

[16] X.H. Li, F.G. Deng, and H.Y. Zhou, “Improving the security of secure direct communication based on the secret transmitting order of particles,” Phys. Rev. A, vol. 74, no. 5, id. 054302, (2006).

[17] Q.Y. Cai, “Eavesdropping on the two-way quantum communication protocols with invisible photons,” Phys. Lett. A, vol. 351, no. 1-2, pp. 23-25, (2006).

# Comment on “Semiquantum secret sharing using entangled states”

Jason Lin, Chun-Wei Yang, Chia-Wei Tsai, and Tzonelih Hwang[*]

**Abstract**

Recently, Li et al. [Phys. Rev. A, 82(2), 022303] presented two semi-quantum secret sharing (SQSS) protocols using GHZ-like states. The proposed schemes are rather practical because only the secret dealer requires to equip with advanced quantum devices such as quantum memory, whereas the other agents can merely perform classical operations to complete the secret sharing. However, this study points out that a security pitfall exists in the eavesdropping check phase of both schemes that could mount to an Intercept-resend attack and a Trojan horse attack on the two schemes, respectively, to disclose the other agent's shadow, and further to reveal the master key of the SQSS, which contradicts to the security requirement of a QSS. Fortunately, two possible solutions are proposed to avoid this security pitfall.

***keywords:*** Quantum secret sharing, GHZ-like state, Intercept-resend attack, Trojan horse attack

## 1 Introduction

Since the first quantum secret sharing (QSS) protocol was presented by Mark et al.'s via triplet Greenberger-Horne-Zeilinger (GHZ) state in 1999 [1], lots of QSS schemes have also been proposed [2-13]. The main goal of a QSS is to distribute a secret among several agents based on the quantum mechanics. Only when enough subsets of legitimate agents cooperate can the

[*] Corresponding Author

secret be recovered. On the contrary, any agent alone is not able to acquire the dealer's secret by his/her own shadow. A secure QSS should be able to avoid the attack from both an outside eavesdropper and an inside malicious user.

Recently, Li et al. proposed two novel semi-quantum secret sharing (SQSS) protocols via triplet GHZ-like state [13]. According to their definition, the term "semi-quantum" implies that the secret dealer is a powerful quantum server, whereas the other agents are all classical clients. More precisely, the secret dealer has the ability to perform the following operations: (1) preparing GHZ-like state, (2) performing the Bell measurement and the three-qubit joint measurement, (3) storing photons in a short-term quantum memory. As for the classical agents, they are restricted to perform the following operations over the quantum channel: (1) preparing new qubits in the classical basis $\{|0\rangle, |1\rangle\}$, (2) measuring photons in the classical basis, (3) reordering the photons via different delay lines, (4) sending or reflecting the qubits without disturbance. Since the classical basis only considers the qubit $|0\rangle$ and $|1\rangle$, the other quantum superpositions of single photon are not included here. Therefore, the agents' operations above are equivalent to the traditional {0, 1} computation.

The two protocols proposed by Li et al. [13] are namely the randomization-based SQSS and the measure-resend SQSS, respectively. Both schemes are based on the entanglement correlation of GHZ-like state $|\psi'\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|\phi^+\rangle + |1\rangle|\psi^+\rangle)$, which can be easily generated by performing the Hadamard gate $H$ $(= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|))$ on each qubit of the standard GHZ state $|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Under the three-party QSS scenario, it can be seen that if each party holds the *1st*, the *2nd*, and the *3rd* particle of a GHZ-like state, respectively, then their classical-basis measurements (say $MR_1$, $MR_2$, and $MR_3$) will agree to a secret sharing relationship: $MR_1 = MR_2 \oplus MR_3$, where the measurement result is encoded as '0' if $|0\rangle$, '1' if $|1\rangle$.

However, this study attempts to show that under the three-party scenario (i.e., one boss and two agents) of Li et al.'s scheme, a malicious agent is possible to launch an Intercept-resend attack on the randomization-based SQSS and a Trojan horse attack [14, 15, 16, 17] on the measure-resend SQSS to reveal the other agent's shadow. This contradicts to the security requirements of a QSS. Fortunately, the above problems can be respectively solved by a carefully designed eavesdropping check process and the use of some special optical devices that filter out the spy photons of the Trojan horse attacks.

The rest of this paper is constructed as follows. Section 2 reviews Li et al.'s two SQSS schemes via GHZ-like state. Section 3 points out the problem and gives two solutions to remedy the loophole. Finally, Section 4 gives a brief conclusion to the result.

## 2 Review of Li et al.'s SQSS schemes

In this section, a brief review of Li et al.'s two SQSS schemes is given. The only difference between these two schemes is the definition of the classical agent's ability. For a randomization-based SQSS protocol, classical agents are limited to perform operations: (2), (3), and (4), while in a measure-resend protocol, classical agents are limited to perform operations: (1), (2), and (4), as defined in Sec. 1.

### 2.1 Randomization-based SQSS protocol

In this subsection, the SQSS is considered under a three-party scenario as follows. Suppose a boss Alice wants to share a secret with her two agents: Bob and Charlie. She splits her secret key $K_A$ into two pieces of shadow key: $K_B$ and $K_C$, which will deliver to Bob and Charlie, respectively. Only when Bob and Charlie collaborate can $K_A$ be recovered. The procedure of the randomization-based SQSS can be described in the following steps:

**Step 1.** Alice first prepares $N$ triplet GHZ-like states all in $|\psi'\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle)$. Here, the quantum states $\{|0\rangle, |1\rangle\}$ can be classically measured by $Z$ basis. Then, she divides these $N$ GHZ-like states into three sequences $S_A$, $S_B$, and $S_C$, which include the *1st*, the *2nd*, and the *3rd* particles of all GHZ-like states, respectively. After the above preparation, Alice retains the quantum sequence $S_A$, and sends the sequence $S_B$ to Bob, $S_C$ to Charlie.

**Step 2.** When Bob and Charlie receive the photons, respectively, they choose to adopt either the SHARE mode or the CHECK mode on each qubit, respectively. In the SHARE mode, the agent performs a $Z$-basis measurement on the qubit, whereas in the CHECK mode, the agent reflects the qubit back to Alice. Notice that those returned qubits in the CHECK mode are reordered via different delay lines.

**Step 3.** Alice stores the reflected qubits from Bob and Charlie in a short-term quantum memory, and publicly announces the reception of these photon sequences. After that, Bob and Charlie publish the correct order of the reflected qubits, and their original positions in the sequences delivered by Alice, respectively. According to the agents' reports, Alice can recover the reflected qubits into the correct order.

**Step 4.** For each GHZ-like state, both Bob and Charlie announce their decisions respectively on the corresponding two particles of $S_B$ and $S_C$, which can be one of the four cases as shown in Table 1. Then, Alice can perform one of the four actions on the corresponding qubits as depicted in Table 1.

**Step 5.** For the eavesdropping check, those qubits in cases (2), (3), and (4) of Table 1 are publicly discussed. The involved parties have to publish their measurement results in those cases to see whether each corresponding three qubits is consistent to the correlation of a GHZ-like state $|\psi'\rangle$ $(= \frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|\phi^{+}\rangle + |1\rangle|\psi^{+}\rangle))$. If the error rate is higher than a predetermined threshold, then Alice terminates the protocol and restarts from Step 1. Otherwise, the protocol continues to the next step.

**Step 6.** As for the secret sharing policy in the case (1) of Table 1, the *1st*, the *2nd*, and the *3rd* qubits of GHZ-like states are measured by Alice, Bob, and Charlie, respectively, using $Z$-basis. They can transform these measurement results into three binary bit sequences, in which the result is '0' if $|0\rangle$ and '1' if $|1\rangle$. After the transformation, Alice, Bob, and Charlie will obtain a key bit string $K_A$, $K_B$, and $K_C$, respectively, which conform to the secret sharing relationship, i.e., $K_A = K_B \oplus K_C$.

Table 1: The actions taken by the secret dealer Alice in each case.

| Case | Bob | Charlie | Alice |
|---|---|---|---|
| (1) | SHARE | SHARE | ACTION (i) |
| (2) | SHARE | CHECK | ACTION (ii) |
| (3) | CHECK | SHARE | ACTION (iii) |
| (4) | CHECK | CHECK | ACTION (iv) |

**(i):** Alice measures her own qubit with $Z$-basis.

**(ii):** Alice performs Bell measurement on her qubit and Charlie's returned qubit.

**(iii):** Alice performs Bell measurement on her qubit and Bob's returned qubit.

**(iv):** Alice performs an appropriate three-qubit joint measurement on her qubit and the returned qubits.

The randomization-based SQSS protocol uses the entanglement correlation of GHZ-like state $|\psi'\rangle$ to achieve the goal of secret sharing. In this type of protocol, the agents will directly perform $Z$-basis measurement on the photons in the SHARE mode. Conversely, by modifying the operations performed by the agents, Li et al. further proposed the other scheme called the measure-resend SQSS protocol, which will be described in Sec. 2.2.

## 2.2 Measure-resend SQSS protocol

Similar to Sec. 2.1, the measure-resend SQSS scheme is also reviewed under a three-party scenario (i.e., a boss Alice, and two agents: Bob and Charlie). The modified steps (*) are depicted in detail as follows. The other steps are the same as those described in Sec. 2.1 and thus are omitted here.

**(*Step 2)** There are two modes (i.e., SHARE and CHECK) that Bob and Charlie can decide to perform on each received photon. For the CHECK mode, the agent still reflects the qubit back to Alice via different delay lines similar to Sec. 1. On the contrary, in the SHARE mode, the agent measures the received qubits in $Z$-basis, and returns a sequence of newly generated photons of the same states to Alice.

**(*Step 3)** Alice stores the photon sequences reflected from Bob and Charlie in a short-term quantum memory, and publicly confirms the reception of them. Subsequently, Bob and Charlie declare the positions of particles being measured and being reflected.

**(*Step 4)** According to the agents' reports, Alice can perform one of the four actions on her own qubit and the corresponding qubits as depicted in Table 1.

The measure-resend SQSS protocol is also based on the entanglement correlation of the GHZ-like state $|\psi'\rangle$. The only difference between these two schemes (the randomization-based SQSS and the measure-resend SQSS) is the type of operations allowed to perform by the agent in the SHARE mode. Considering the eavesdropping check, both schemes discuss the measurement result of each qubit in the GHZ-like state to detect the presence of eavesdroppers. However, this check strategy may not be able to prevent Bob or Charlie from maliciously launching attacks on the SQSS protocols. More details of the attacks will be discussed in Sec. 3.

# 3 Attacks and the improvements

This section shows that under the three-party scenario (i.e., one boss and two agents) of Li et al.'s scheme, a malicious agent is possible to launch an Intercept-resend attack on the randomization-based SQSS and a Trojan horse attack [14, 15, 16, 17] on the measure-resend SQSS to reveal the other agent's shadow and further to derive Alice's secret key. This contradicts to the security requirements of a QSS. Fortunately, the above problems can be respectively solved by a carefully designed eavesdropping check process and the use of some special optical devices that filter out the spy photons of the Trojan horse attacks.

## 3.1 Attacks on Li et al.'s SQSS schemes

Both Bob and Charlie can act as a dishonest insider to derive Alice's shared secret. In general, an eavesdropper is assumed to be powerful enough to equip with any quantum devices [18, 19, 20]. Hence, the malicious classical agent is able to perform any operation as defined in Sec. 1.

### 3.1.1 The Intercept-resend attack on the randomization-based SQSS.

Suppose that Bob is a dishonest insider. He first intercepts the photon sequence $S_C$ (from Alice to Charlie) in Step 1, and stores it in his quantum memory. Then, he prepares a new photon sequence $S_E$ randomly chosen from $|0\rangle$ or $|1\rangle$, and sends it to Charlie, where $S_E$ is of the same length as $S_C$. Notice that the wavelength of each photon in $S_E$ is set to be different from the others so that Bob is alble to identify their individual position.

When Charlie receives the sequence $S_E$ in Step 2, he will perform $Z$-basis measurement on those photons chosen for the SHARE mode, and reflect the ones that are chosen for the CHECK mode via different delay lines. At this time, Bob can intercept the reflected sequence (from Charlie to Alice), and replace those photons with the corresponding photons in $S_C$ and then send them back to Alice. Bob is able to do so by distinguishing the wavelengths of the reflected photons from Charlie.

Later, Bob deliberately selects the SHARE mode on those photons in $S_B$ that their corresponding photons in $S_C$ have been chosen by Charlie as in the SHARE mode, and randomly select SHARE or CHECK on the other photons in $S_B$. The above action is to avoid the presence of the case (3) in Table 1 because it has a 50% probability of being detected. More precisely, since all the SHARE photons measured by Charlie are the forged photons in $S_E$, there is a 50% probability on each three-particle set of the case (3) that will not follow the entanglement correlation of GHZ-like state $|\psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\phi^+\rangle + |1\rangle|\psi^+\rangle)$.

For the eavesdropping check, Bob can escape from detection because of all the reflected photons in cases (1), (2), and (4) of Table 1 are indeed generated by Alice. Therefore, he can obtain Charlie's shadow $K_C$ by measuring the SHARE photons in $S_C$, and further derive Alice's secret key with $K_B \oplus K_C = K_A$.

### 3.1.2 The Trojan-horse attack on the measure-resend SQSS.

Let us also assume here that Bob is a malicious insider. He first attaches some invisible photons [15, 17] $S_T$ on each particle of $S_C$ transmitted from Alice to Charlie in Step 1, and then inserts some delay photons [15, 16] $S_D$ in the same time window to each particle of $S_C$. Notice that the wavelength in each photon of $S_D$ is set to be the same as the corresponding photon in $S_C$, whereas the wavelength in each photon of $S_T$ is close to the corresponding photon in $S_C$.

When Charlie receives the sequence $S_C$ in Step 2, he measures those photons in the SHARE mode with $Z$-basis, and returns a sequence of newly generated photons of the same states to Alice. The corresponding photons of the SHARE photons in $S_T$ and $S_D$ will vanish after the replacement of the newly produced photons. As for the CHECK photons, Charlie will directly reflect them without any reordering operation to Alice. At this time, Bob can intercept the returned sequence (from Charlie to Alice), and perform $Z$-basis measurement on those photons that their corresponding spy photons have disappeared.

After the measurement, Bob resends the returned sequence back to Alice without any further action. Since Alice will also perform $Z$-basis measurement on the SHARE photons of Charlie in Step 4, the measurement results will not be different from the ones measured by Bob. Hence, the three cases (1), (2), and (3) in Table 1 used for the eavesdropping check will not detect the attack. Bob can obtain Charlie's shadow $K_C$ by those $Z$-basis measurement results of the SHARE photons in the case (4) of Table 1 and further derive Alice's secret key with $K_B \oplus K_C = K_A$.

## 3.2 Possible solutions for the attacks

Two solutions to avoid the attacks are proposed here. The first one is to set a new threshold of eavesdropping check in the randomization-based SQSS. The second solution is to equip with some special optical filter devices to detect the Trojan horse attacks on the measure-resend SQSS.

**Solution 1.** A new threshold for the eavesdropping check.

In Table 1, all four cases should be evenly distributed. However, if Bob performs the intercept-resend attack as shown in Sec. 3.1.1, there is no chance for case (3) of Table 1 to appear. Thus, to prevent this attack, before the eavesdropping check of Step 5, Alice can first calculate the occurrence $\rho$ of case (3) in Table 1, and decide the existence of the attack. If $\rho$ is too small, then Alice can abort the protocol.

**Solution 2.** Agents install some optical filter devices.

Since the attack in Sec. 3.1.2 is based on the spy photons in the Trojan horse attacks, when Charlie receives the photons in Step 2, he can equip with some special optical devices such as the wavelength quantum filter and the photon number splitters (PNS) to detect the attacks. According to [14, 15, 16, 17], the wavelength quantum filter can eliminate the invisible photons attached on the legitimate ones, and the PNS can spit each legitimate particle to discover the delay photons. If there is an irrational high rate of multi-photon signal, then Charlie announces to restart the protocol from Step 1.

## 4 Conclusions

This paper has pointed out two attacks on both of Li et al.'s SQSS schemes, respectively. Under the three-party scenario (i.e., one boss and two agents), a malicious insider could possibly launch the Intercept-resend attack on the randomization-based SQSS and the Trojan horse attacks on the measure-resend SQSS to obtain the other agent's shadow, which can also lead to derive the boss's secret key. Fortunately, two solutions are given in this paper to avoid the attacks (i.e., one is to add a new threshold for the eavesdropping check, and the other is to equip with some special optical devices to filter out the spy photons). With the second solution, since near a half of the transmitted photons are used in devices to detect the Trojan horse attack for each agent, the qubit efficiency will be seriously jeopardized. Hence, how to design a QSS protocol which is congenitally free from this attack is a promising future research.

## Acknowledgement

We would like to thank the National Science Council of the Republic of China, Taiwan for partially supporting this research in finance under the Contract No. NSC 98-2221- E-006-097-MY3.

# References

[1] M. Hillery, V. Bužek, and A. Berthiaume, “Quantum secret sharing,” Phys. Rev. A, vol. 59, no. 3, pp. 1829-1834, (1999).

[2] D. Gottesman, “Theory of quantum secret sharing,” Phys. Rev. A, vol. 61, no. 4, id. 042311, (2000).

[3] G.P. Guo and G.C. Guo, “Quantum secret sharing without entanglement,” Phys. Lett. A, vol. 310, no. 4, pp. 247-251, (2003).

[4] L. Xiao, G.L. Long, F.G. Deng, and J.W. Pan, “Efficient multiparty quantum-secret-sharing schemes,” Phys. Rev. A, vol. 69, no. 5, id. 052307, (2004).

[5] L.Y. Hsu and C.M. Li, “Quantum secret sharing using product states,” Phys. Rev. A, vol. 71, no. 2, id. 022321, (2005).

[6] Z.J. Zhang and Z.X. Man, “Multiparty quantum secret sharing of classical messages based on entanglement swapping,” Phys. Rev. A, vol. 72, no. 2, id. 022303, (2005).

[7] F.G. Deng, G.L. Long, and H.Y. Zhou, “An efficient quantum secret sharing scheme with Einstein-Podolsky-Rosen pairs,” Phys. Lett. A, vol. 340, no. 1-4, pp. 43-50, (2005).

[8] F.G. Deng, X.H. Li, and H.Y. Zhou, “Efficient high-capacity quantum secret sharing with two-photon entanglement,” Phys. Lett. A, vol. 372, no. 12, pp. 1957-1962, (2008).

[9] Y. Sun, Q.Y. Wen, F. Gao, X.B. Chen, and F.C. Zhu, “Multiparty quantum secret sharing based on Bell measurement,” Opt. Commun., vol. 282, no. 17, pp. 3647-3651, (2009).

[10] J.H. Chen, K.C. Lee, and T. Hwang, “The enhancement of Zhou et al.’s quantum secret sharing protocol,” Int. J. Mod. Phy. C, vol. 20, no. 10, pp. 1531-1535, (2009).

[11] R.H. Shi, L.S. Huang, W. Yang, and H. Zhong, “Multiparty quantum secret sharing with Bell states and Bell measurements,” Opt. Commun., vol. 283, no. 11, pp. 2476-2480, (2010).

[12] C.R. Hsieh, C.W. Tsai, and T. Hwang, “Quantum secret sharing using GHZ-like state,” Commun. Theor. Phys., vol. 54, no. 6, pp. 1019-1022, (2010).

[13] Q. Li, W.H. Chan, and D.Y. Long, “Semiquantum secret sharing using entangled states,” Phys. Rev. A, vol. 82, no. 2, id. 022303, (2010).

[14] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys., vol. 74, no. 1, pp. 145-195, (2002).

[15] F.G. Deng, X.H. Li, H.Y. Zhou, and Z.J. Zhang, “Improving the security of multiparty quantum secret sharing against Trojan horse attack,” Phys. Rev. A, vol. 72, no. 4, id. 044302, (2005).

[16] X.H. Li, F.G. Deng, and H.Y. Zhou, “Improving the security of secure direct communication based on the secret transmitting order of particles,” Phys. Rev. A, vol. 74, no. 5, id. 054302, (2006).

[17] Q.Y. Cai, “Eavesdropping on the two-way quantum communication protocols with invisible photons,” Phys. Lett. A, vol. 351, no. 1-2, pp. 23-25, (2006).

[18] H.K. Lo and H.F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” Science, vol. 283, no. 5410, pp. 2050-2056, (1999).

[19] K. Bostroem and T. Felbinger, “Deterministic secure direct communication using entanglement,” Phys. Rev. Lett., vol. 89, no. 18, id. 187902, (2002).

[20] Y. Sun, Q.Y. Wen, and F.C. Zhu, “Improving the multiparty quantum secret sharing over two collective-noise channels against insider attack,” Opt. Commun., vol. 283, no. 1, pp. 181-183, (2010).